UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,192	10/21/2003	Brant L. Candelore	80398P558X	3671

8791 7590 03/12/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
MORAN, RANDAL D	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/690,192	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/21/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :3/25/2004, 2/39/2004, 9/27/2004, 9/27/2004, 9/29/2004, 1/3/2005, and 12/11/2006.

DETAILED ACTION

1. Claims 1-31 are pending in this application.

2. The information disclosure statements filed on 3/25/2004, 2/39/2004, 9/27/2004, 9/27/2004, 9/29/2004, 1/3/2005, and 12/11/2006 have been considered by the examiner.

Drawings

3. The drawings are objected to because Figure 25, which is considered to be the overview of the entire invention, does not show the second cryptographic unit **1160**. Examiner believes this should be labeled as containing the CP Decryption Logic 1150 in Figure 25. Corrected drawing sheets are required. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 6, 8, 10-13, 18, 19, 22, and 28 are rejected under 35 U.S.C. 102(b) as being anticipated by **Wasilewskiewski et al. (US 2002/0094084)**, hereafter "Wasilewskiewski."

6. Considering **Claims 1 and 13,** Wasilewski discloses descrambler (abstract- lines 1-7) comprising: a non-volatile memory to store a unique key (Fig. 3- item 400); a control word key ladder logic (Fig. 3, Fig. 3A) to produce (i) a first value generated based on a conditional access (CA) random value and the unique key ([0053] lines 1-6, Fig. 3A- item 20, other data, the control word, and the MSK are concatenated together to form a first value), (ii) a second value generated using the first value ([0053] lines 6-17, Figure 3A- item 1004 and MAC), and (iii) a third value recovered using the second value ([0054] lines 1-9, Figure 3A- item 1008 and Clear CW); a first cryptographic unit to descramble incoming content in a scrambled format based on the third value (Fig. 3A- item 1008, [0054] lines 1-9);

and a second cryptographic unit to decrypt incoming encrypted data using the first value (Fig. 3A- item 1012 and MAC, the MAC is compared to the hash value and then used to decrypt the program, [0054] lines 9-12).

7. Considering **Claim 22,** Wasilewski discloses a descrambler comprising: a memory to store a unique key ([0057] lines 1-10, the key is implanted during manufacture); a control word key ladder logic coupled to the memory ([0053] lines 1-17), the control word ladder logic comprising a first process block configured to generate a first derivative key of the unique key ([0053] lines 1-6), a second process block configured to generate a mating key from a mating key generator using the first derivative key ([0053] lines 6-17), and a third process block configured to recover a control word by decrypting an encrypted control word using the mating key ([0054] lines 1-9); a first cryptographic unit coupled to the control word key ladder logic (Fig. 3A- item 1008, [0054] lines 1-9); the first cryptographic unit to descramble incoming content in a scrambled format using the control word (Fig. 3A- item 1012 and MAC).

8. Considering **Claim 28,** Wasilewski discloses a descrambler comprising: a non-volatile memory to store a plurality of unique keys ([0057] lines 1-10, the key is implanted during manufacture); a control word key ladder logic to produce (i) a plurality of derivative keys generated based on a conditional access (CA) random value and a corresponding plurality of unique keys ([0053] lines 1-6), (ii) a

plurality of mating keys generated using the plurality of derivative key ([0053] lines 6-17), and (iii) a plurality of control words recovered using the plurality of mating keys ([0054] lines 1-9); and a first cryptographic unit to descramble incoming content in a scrambled format based on at least one of the plurality of control words (Fig. 3A- item 1012 and MAC).

9. Considering **Claim 2, 14, and 23,** Wasilewski discloses descrambler of claim 1 being a single integrated circuit. It is inherent that the Wasilewski reference would be implemented using a single integrated circuit.

10. Considering **Claim 3,** Wasilewski discloses descrambler of claim 1 implemented within a set-top box ([0033] lines 9-17).

11. Considering **Claim 4,** Wasilewski discloses the first value is a derivative key generated by performing a decryption operation on the CA random value using the unique key ([0053] lines 1-6, Fig. 3A- item 20, the decryption operation is that the copy protection data is decrypted and used in the concatenation to produce first value).

12. Considering **Claim 6,** Wasilewski discloses the second value is a mating key recovered by performing a decryption operation on a mating key generator using the derivative key ([0053] lines 6-17, Fig. 3A- item 1004, MAC), the mating key

generator being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number ([0057] lines 1-10).

13. Considering **Claim 8,** Wasilewski discloses the third value is a control word recovered by performing a decryption operation on an encrypted control word using the mating key ([0054] lines 1-9, Fig. 3A- item 1008, Clear CW).

14. Considering **Claim 10,** Wasilewski discloses a third cryptographic unit to encrypt the descrambled incoming content prior to transmission to a digital device (Figure 3A- item 1010).

15. Considering **Claim 11,** Wasilewski discloses a copy protection ladder logic to produce a copy protection key used by the third cryptographic unit to encrypt the descrambled incoming content ([0053] lines 1-9).

16. Considering **Claim 12,** Wasilewski discloses the copy protection ladder logic to produce a copy protection key by performing a decryption operation on a concatenation of a random value and a plurality of bits to produce a result being at least 128-bits in length, using a logical derivation being a result of an Exclusive OR (XOR) operation of the unique key and a predetermined value ([0053] lines 1-17, Fig. 3A, Fig 4- item 220).

17. Considering **Claim 18,** Wasilewski discloses a copy protection ladder logic to produce a copy protection key based on a plurality of process blocks (Fig. 3), wherein a first process block configured to generate a derivative key based on a second random value and either the unique key or a logical derivation of the unique key ([0053] lines 1-6, Fig. 3A), a second process block configured to recover a user key from an encrypted user key using the derivative key ([0053] lines 6-17, Fig. 3A), and a third process block configured to generate a copy protection key from a copy protection key generator using the user key ([0054] lines 1-9).

18. Considering **Claim 19,** Wasilewski discloses a third cryptographic unit to encrypt the descrambled incoming content using the copy protection key prior to transmission to a digital device ([0053] lines 1-9, [0054] lines 1-9).

19. Considering **Claim 29,** is rejected for the same reasons as claim 1 stated above. The ability to create a first key makes it obvious to create a second and third key using the same logic.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. **Claims 5, 7, 9, 20, 21, 26, and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski**.

22. Considering **Claim 5,** Wasilewski discloses the first value is a derivative key derived by performing a decryption operation on a combination of the CA random value and padding data ([0053] lines 1-6), the combination being at least 128-bits in length ([0046] lines 6-8, [0049] lines 9-13, [0050] lines 15-20, Fig. 4- item 220). Official notice is taken that it would have been obvious to one of ordinary skill in the art at the time of the invention to pad the data to 128 bits for the benefit of increasing the security of the conditional access system.

23. Considering **Claim 7,** Wasilewski discloses the second value is a mating key recovered by performing a decryption operation on at least 128-bits of data ([0053] lines 6-17, Fig. 3A- item 1004, MAC) comprising a mating key generator being a message comprising one or more of the following: a manufacturer

identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number ([0057] lines 1-10).

24. Considering **Claim 9,** Wasilewski discloses the third value is a control word recovered by performing (i) a first decryption operation using the mating key on a first combination of a first encrypted control word and a second encrypted control word ([0054] lines 1-9, Fig. 3A- item 1008, Clear CW), and (ii) a second decryption operation using the mating key on a second combination of a third encrypted control word and a plurality of bits operating as padding for the second combination to be at least 128-bits in length ([0053] lines 1-6, Fig. 4- item 20).

25. Considering **Claim 20 and 21,** Wasilewski does not explicitly discloses a one-time programmable, non-volatile memory coupled to the control word key ladder logic and the copy protection ladder logic, the non-volatile memory to store the unique key. Official notice is taken that it would have been obvious to one of ordinary skill in the art at the time of the invention to store the unique key on a one-time programmable, non-volatile memory for the benefit of not allowing the unique key to be tampered with or overwritten.

26. Considering **Claim 26,** Wasilewski does not explicitly disclose a copy protection ladder logic coupled to the first cryptographic unit, the copy protection ladder logic comprising a fourth process block configured to generate a second

derivative key based on a random value and the unique key; a fifth process block configured to decrypt an encrypted user key using the second derivative key to recover a user key; and a sixth process block configured to generate a copy protection key from a copy protection key generator using the user key. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Wasilewski by adding a 4^{th}-6^{th} process block for the benefit of further encrypting the data and increasing the security of the unit.

27. Considering **Claim 27,** Wasilewski discloses a second cryptographic unit to encrypt the descrambled incoming content using the copy protection key prior to transmission to a digital device (Fig. 3A- item 90 and 1008).

28. **Claims 15-17, 24, 25, 30, 31, and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wasilewski in view of Wasilewski (US 2004/003008),** hereafter `008.

29. Considering **Claims 15 and 24,** Wasilewski does not explicitly disclose a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler.

`008 does explicitly disclose a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler ([0013]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Wasilewski by encrypting data received out-of-band as taught by `008 in order to encrypt incoming authorization information ([0013]).

30. Considering **Claim 16 and 25,** Wasilewski discloses the encrypted program data comprises an encrypted entitlement management message that comprises at least two of (i) a smart card identifier, (ii) a length field, (iii) a mating key generator, (iv) at least one key identifier and (v) at least one key associated with the at least one key identifiers ([0062]).

31. Considering **Claim 17,** Wasilewski discloses where the mating key generator of the encrypted entitlement management message being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number ([0062]).

32. Considering **Claim 30,** is rejected for the same reasons as claims 13-16 stated above. The ability to perform the same transformation multiple times would have been obvious to one of ordinary skill in the art.

33. Considering **Claim 31,** is rejected for the same reasons as claims 22-27 stated above. The ability to perform the same transformation multiple times would have been obvious to one of ordinary skill in the art.

34. Considering **Claim 32,** Wasilewski discloses the bitwise logical operation is an Exclusive OR operation ([0053] lines 6-11).

Conclusion

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 6,157,719- a previous Wasilewski reference.
- US 2003/0108199- Set-Top-Box encryption method
- US 2002/0090090- Conditional Access System.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
RDM
3/6/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100